PARAS PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

PARAS 0060 July 2024

Strategies for Developing an Aviation Worker Screening Program

National Safe Skies Alliance, Inc.

Sponsored by the Federal Aviation Administration

Neil Trethewey
Michele Freadman
Kim Dickie
Craig Lynes
Rose Marengo
LAM LHA USA LLC
Washington, DC

NOTICE

The project that is the subject of this report was a part of the Program for Applied Research in Airport Security (PARAS), managed by Safe Skies and funded by the FAA.

The members of the technical panel selected to monitor this project and to review this report were chosen for their special competencies and with regard for appropriate balance. The report was reviewed by the technical panel and accepted for publication according to procedures established and overseen by Safe Skies.

The opinions and conclusions expressed or implied in this report are those of the individuals or organizations who performed the research and are not necessarily those of Safe Skies or the FAA.

Safe Skies and the FAA do not endorse products or manufacturers.

NATIONAL SAFE SKIES ALLIANCE, INC.

National Safe Skies Alliance (Safe Skies) is a non-profit organization that works with airports, government, and industry to maintain a safe and effective aviation security system. Safe Skies' core services focus on helping airport operators make informed decisions about their perimeter and access control security.

Through the ASSIST (Airport Security Systems Integrated Support Testing) Program, Safe Skies conducts independent, impartial evaluations of security equipment, systems, and processes at airports throughout the nation. Individual airports use the results to make informed decisions when deploying security technologies and procedures.

Through the POST (Performance and Operational System Testing) Program, Safe Skies conducts long-term evaluations of airport-owned equipment to track and document a device or system's performance continuously over its life cycle.

Through PARAS (Program for Applied Research in Airport Security), Safe Skies provides a forum for addressing security problems identified by the aviation industry.

A Board of Directors and an Oversight Committee oversee Safe Skies' policies and activities. The Board of Directors focuses on organizational structure and corporate development; the Oversight Committee approves PARAS projects and sets ASSIST Program priorities.

Funding for our programs is provided by the Federal Aviation Administration.

PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

The Program for Applied Research in Airport Security (PARAS) is an industry-driven program that develops near-term practical solutions to security problems faced by airport operators. PARAS is managed by Safe Skies, funded by the Federal Aviation Administration, and modeled after the Airport Cooperative Research Program of the Transportation Research Board.

Problem Statements, which are descriptions of security problems or questions for which airports need guidance, form the basis of PARAS projects. Submitted Problem Statements are reviewed once yearly by the Safe Skies Oversight Committee but can be submitted at any time.

A project panel is formed for each funded problem statement. Project panel members are selected by Safe Skies, and generally consist of airport professionals, industry consultants, technology providers, and members of academia—all with knowledge and experience specific to the project topic. The project panel develops a request of proposals based on the problem statement, selects a contractor, provides technical guidance and counsel throughout the project, and reviews project deliverables.

The results of PARAS projects are available to the industry at no charge. All deliverables are electronic, and most can be accessed directly at www.sskies.org/paras.

PARAS PROGRAM OFFICER

Jessica Grizzle *Safe Skies PARAS Program Manager*

PARAS 0060 PROJECT PANEL

Nicholas Bryant F*t. Lauderdale-Hollywood International Airport*
Lisa Carr *Gerald R. Ford International Airport*
Aimee Crook *Jackson Hole Airport*
Matt Dowell *Golden Triangle Regional Airport*
Jessica Gafford *TranSolutions, LLC*
Tricia Harder *Omaha Airport Authority*
Raymond Hunting *Hollywood Burbank Airport*
Richard King *Sioux Falls Regional Airport*
Bonnie Kudrick *HumanLink, LLC*
Terry McHugh *Seattle-Tacoma International Airport*
Sean Michael *Portland International Airport*
Cedric Simon *Lynchburg Regional Airport*
Jodi Spencer *Boise Airport*

AUTHOR ACKNOWLEDGMENTS

The research conducted for this guidebook was performed by LAM LHA USA LLC (LAM LHA) with the assistance of M. Freadman Consulting, LLC and KPD Consulting, LLC.

Neil Trethewey with LAM LHA was the Principal Investigator for the project. Anne Marie Pellerin, Craig Lynes, and Rose Marengo, also with LAM LHA; Michele Freadman with M. Freadman Consulting; and Kim Dickie with KPD Consulting assisted with the research, facilitation of the airport discussion groups, and editing.

The Research Team would like to acknowledge the airports that participated in the airport discussion groups and provided relevant strategies and practices to support the development of this guidebook. It is only through the participation of airports that Safe Skies is able to continue to provide the aviation industry with valuable research on practical airport-related topics.

Finally, the Research Team would like to thank Safe Skies and the project panel for their support and expertise throughout the research process to ensure the guidebook is useful and applicable.

Airport Discussion Group Participants

- Baltimore/Washington International Thurgood Marshall Airport
- Bangor International Airport
- Boise Airport
- Charlotte Douglas International Airport
- Denver International Airport
- Eastern Iowa Airport
- Eugene Airport
- Fort Lauderdale–Hollywood International Airport
- Gerald R. Ford International Airport
- Port Authority of New York & New Jersey
- Oakland International Airport
- Omaha-Eppley Airfield
- Ontario International Airport
- Phoenix Sky Harbor International Airport
- San Diego International Airport
- San Francisco International Airport
- Seattle-Tacoma International Airport
- Sioux Falls Regional Airport
- Washington Dulles International Airport
- Westchester County Airport

CONTENTS

TABLES & FIGURES

SUMMARY

This guidebook is a practical resource for airport operators across the United States to use when planning for and integrating aviation worker screening (AWS) into airport operations. It provides airport operators and their partners with a suite of information, strategies, and options to support the implementation of AWS at their airports and achieve a positive security outcome. These solutions are summarized below.

Focus Area	Considerations and Options
Evaluating Access Points	Space, infrastructure, and operations may be the deciding factors for many airport operators, given the limited space before access points or infrastructure not being available, and the goal of avoiding operational impacts related to AWS. Consultation and coordination with the stakeholders, local TSA, and local police are all highly recommended. Conducting screening **before** the access point will require TSA approval. A benefit of screening before the access point is that alarms and issues can be resolved alarms prior to the entry into the Secured or Sterile Area.
Staffing Models (direct airport employees, security contractors, hybrid, airport law enforcement)	Four options for staffing AWS checkpoints or access points include the following: **Direct Airport Employees:** The airport directly hires and manages the screening staff. This provides for efficient deployment, flexibility to cross-utilize job roles, and greater control over job performance. However, it may come with higher costs because of fully loaded salary and benefits, higher turnover of personnel, a less experienced workforce, and possible labor union engagement. **Security Contractors:** The airport hires a security company that provides the screening staff. This option generally has greater screening capability with experienced/trained personnel, easier recruitment and deployment of resources, flexibility without full-time employee obligations, and relieves the airport of performing personnel responsibilities associated with direct employees. **Hybrid:** By combining direct airport employees and security contractors, airports can adjust staffing based on security needs and budget constraints. Under this model, airports generally perform oversight and management responsibilities of the contractor to ensure adherence to the contract. **Airport Law Enforcement:** This model is an uncommon approach, but has advantages of leveraging law enforcement capabilities, including their legal powers to streamline incident response and alarm resolution.
Screening Methods (manual vs. technological)	Airports with a high number of public-to-Secured Area and public-to-Sterile Area access points should consider manual screening until the TSA Explosive Detection Screening Equipment (EDSE) requirement is implemented. • The most practical solution is the establishment of an AWS program using handheld metal detectors and stadium-style searches of bags and accessible property. Using technology in the screening process can enhance threat detection accuracy and ensure a higher level of assurance that prohibited items are detected in the screening process.

	TSA provides a list of screening equipment that is available on the Homeland Security Information Network (HSIN), with several products showcased for AWS. Airport operators should consider using CCTV cameras to monitor the AWS process from all views. This is important for ensuring compliance, providing audit and quality assurance capabilities, and reducing complaints and liability claims.
Establishing Standard Operating Procedures (including alarm resolution)	Airport operators can develop their SOPs internally, outsource to their security contractor, or use a combination of both approaches. Some airports will provide the program requirements to their security contractor and delegate the responsibility of drafting SOPs while performing oversight functions and retaining final approval authority. Airport operators governed by city, local, or state government agencies should assess the potential time considerations and delays to develop, review, approve, and implement new procedures for their airport community. Early involvement and coordination with key stakeholders (e.g., legal, risk management, law enforcement, TSA) to develop effective SOPs is paramount for a successful AWS program. A "no touch" policy for AWS is a common practice at airports to reduce litigation risks, including challenges when attempting to resolve alarms activated during the screening process. Airports have two options for scheduling AWS: 1. Use TSA's Random Screening Scheduler (RSS). 2. Develop an airport-generated schedule, approved by TSA, that may include the Enhanced Scheduling Tool for AWS discussed in Safe Skies PARAS 0059. This tool is available upon request to Safe Skies. Airports should include procedures to manage and report the detection of prohibited items (as defined by the airport), unauthorized weapons, explosives, and/or incendiaries, as required by the National Amendment. SOPs will need to incorporate processes authorizing tools of the trade and other items that are prohibited but have an operational need. In addition to development, SOPs will need to be coordinated with the workforce, law enforcement, and TSA. Socialization of the procedures and training is necessary for both the aviation workers and personnel responsible for conducting AWS.
Prohibited Items	Airports have several options to develop and establish a Prohibited Items List (PIL): • Use the TSA's Passenger Screening PIL • Develop one list for Secured Areas and another for Sterile Areas • Develop a Dangerous Items or Restricted Items List • Adopt a hybrid list of prohibited items • Consult with legal counsel, airport law enforcement, and TSA to ensure alignment of the airport's PIL • International Civil Aviation Organization (ICAO) offers an example PIL

	Tools of the trade: • Seek input from airport stakeholders on tools of the trade or items with an operational need, and coordinate with TSA on these items as feasible • Identify aviation workers who have an operational and lawful purpose to carry tools of the trade into a Secured or Sterile Area is needed Strategies for addressing tools of the trade may include: • Airport ID/badge endorsement (e.g., tool icon) • Tool inventory forms and approvals
Communicating with Stakeholders	Airport operators should leverage the support of senior executives to communicate with stakeholders about AWS. Airport operators should consider using multiple channels to notify and inform aviation workers of screening requirements. These may include: • Publications, including newsletters • Social media • Committees, forums, and meetings • Training • Airport apps accessible to stakeholders • Badging materials and acknowledgments, in addition to the required TSA language in the badge application • Communication and education provided by personnel conducting AWS screening to the individuals being screened • Rules and regulations specific to AWS • Airport operator's ID media and SIDA training
Recordkeeping and Reporting	Airport operators, familiar with record retention requirements, record availability, and TSA inspection authority, must comply with the recordkeeping requirements in the NA and may use a variety of options. Airport operators may have different reporting requirements for the daily AWS statistics, as agreed upon by the TSA FSD or their designee. Early coordination with the TSA FSD is recommended.
Cost Considerations	The NA that mandates AWS is unfunded. Costs will include operating and capital expenses, direct and indirect costs, and operation and maintenance contracts, which require multiple-year planning for budgets, procurement, and contracts. Personnel costs are typically among the most significant costs for direct airport employees and contractors. Direct costs may include: • Screening equipment, including the future EDSE requirement • Personnel • Consumables, including disposable swabs for explosives trace detection (ETD) • Infrastructure • Security technology • Training

	Indirect costs (ongoing) may include: • Insurance • Equipment maintenance • Employee expenses AWS will be an expensive undertaking for many airports. Finding the necessary funds within existing budgets and educating executives about this mandatory requirement may be challenging. The earlier the budget and financial aspects of AWS are considered in the planning process, the better the airport operator will be positioned to fund the operation. In acquiring screening equipment, it is important to understand the airport procurement procedures and requirements and program these costs in the budget cycle.
Legal Considerations	Airport operators should consider contractors who have received DHS Safety Act Certification or Designation to mitigate risk in the performance of their duties. Airport operators raised questions about responsibilities, the discovery of prohibited items, and compliance matters. Airport operators seek to limit their liabilities related to AWS by working closely with the following internal and external stakeholders to evaluate the most appropriate AWS procedures, policies, and options for their airport: • Legal counsel • Risk management • Airport law enforcement officials • TSA officials

PARAS ACRONYMS

ACRP	Airport Cooperative Research Program
AIP	Airport Improvement Program
AOA	Air Operations Area
ARFF	Aircraft Rescue & Firefighting
CCTV	Closed-Circuit Television
CFR	Code of Federal Regulations
DHS	Department of Homeland Security
DOT	Department of Transportation
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FSD	Federal Security Director
GPS	Global Positioning System
IED	Improvised Explosive Device
IT	Information Technology
MOU	Memorandum of Understanding
RFP	Request for Proposals
ROI	Return on Investment
SIDA	Security Identification Display Area
SOP	Standard Operating Procedure
SSI	Sensitive Security Information
TSA	Transportation Security Administration

ABBREVIATIONS, ACRONYMS, INITIALISMS, AND SYMBOLS

AAAE	American Association of Airport Executives
ASP	Airport Security Program
ASSIST	Airport Security Systems Integrated Support Testing
AWS	Aviation Worker Screening
EAA	Exclusive Area Agreement
EDSE	Explosive Detection Screening Equipment
ETD	Explosives Trace Detection
FTE	Full-Time Equivalent
HHMD	Handheld Metal Detector
HSIN	Homeland Security Information Network
ICAO	International Civil Aviation Organization
NA	National Amendment
PIL	Prohibited Items List
QR	Quick Response
RSS	Random Screening Scheduler
SPP	Screening Partnership Program
WTMD	Walk-Through Metal Detector

SECTION 1: GUIDEBOOK OVERVIEW

The threat posed by aviation insiders is a long-standing and enduring security risk. TSA and International Civil Aviation Organization (ICAO) have discussed approaches and standards to conduct aviation worker screening (AWS) in a manner that effectively mitigates insider threat.

In April 2023, TSA issued a National Amendment (NA) for Airport Security Programs (ASP) that requires specific categories of US airport operators to enhance screening of aviation workers.[1] AWS is intended to deter insider threats at airports by establishing an expectation that aviation workers could be screened any time they enter a Secured or Sterile Area from a public area of the passenger terminal. Although TSA has levied a mandate, there is minimal guidance available to assist airports with the implementation of this undertaking. Key challenges for airport operators impacted by the NA include:

- Airport operators must strengthen or create policies, procedures, and processes to meet TSA's new requirements. In addition, they will need to effectively communicate these changes to aviation workers and mitigate liability where possible.
- Most airport operators do not own screening equipment, nor do they have sufficient personnel to undertake these activities. These airports will have to develop requirements, procurement strategies, and contractual relationships with technology manufacturers and security personnel providers.
- Airport operators must identify solutions to fund these AWS activities and equipment.

This research was designed to provide airports with information regarding the key components of an AWS program that can be used during program planning, development, implementation, and refinement.

1.1 Research Approach

LAM LHA conducted airport discussion groups with 20 US airport operators to acquire knowledge, strategies, and guidance to assist airport operators in developing and implementing an AWS program that complies with the TSA NA:

- Baltimore/Washington International Thurgood Marshall Airport
- Bangor International Airport
- Boise Airport
- Charlotte Douglas International Airport
- Denver International Airport
- Eastern Iowa Airport
- Eugene Airport
- Fort Lauderdale-Hollywood International Airport
- Gerald R. Ford International Airport
- Port Authority of New York & New Jersey
- Oakland International Airport
- Omaha-Eppley Airfield
- Ontario International Airport
- Phoenix Sky Harbor International Airport
- San Diego International Airport
- San Francisco International Airport
- Seattle-Tacoma International Airport
- Sioux Falls Regional Airport
- Washington Dulles International Airport
- Westchester County Airport

[1] The NA also applies to aircraft operators and foreign air carriers that hold an Exclusive Area Agreement (EAA) under 49 CFR §§ 1542.111 and 1544.227. This document addresses airport operators directly, but the guidance may also apply to EAA holders as determined in coordination with their respective airports.

Each of the four airport discussion groups was facilitated by two US airport industry experts. The output from these sessions provided the project team with key strategies, considerations, and critical decision points to be used in the development of the guidebook. In addition, one-on-one interviews were held with several airport operators to clarify information and obtain additional details related to topics covered in the discussion groups.

Based on the results of the airport discussion groups and interviews, this guidebook addresses the following topics:

Section 2: Evaluating Access Points
This section discusses evaluating access points, including determining the number used, addressing closures, and designing the screening process to meet operational and footprint requirements.

Section 3: Staffing Models
This section addresses the various staffing models (direct airport employees, security contractor, hybrid, airport law enforcement) to conduct AWS and outlines the advantages and disadvantages of each model.

Section 4: Screening Methods
This section describes manual and technology-based screening methodologies to consider.

Section 5: Establishing Standard Operating Procedures
This section discusses roles and responsibilities to develop, implement, and manage operating procedures.

Section 6: Prohibited Items
This section outlines designing a Prohibited Items List (PIL; inclusive of tools of trade) and notification, education, and operational requirements.

Section 7: Communicating with Stakeholders
This section addresses communicating with stakeholders and strategies to establish a reasonable expectation of being screened.

Section 8: Recordkeeping and Reporting
This section addresses reporting requirements as per TSA regulations, NA-23-02 and 49 CFR § 1542.5.

Section 9: Cost Considerations
This section outlines expected cost implications in the development and implementation of AWS.

Section 10: Legal Considerations
This section discusses potential legal issues and challenges for airport operators to consider in their AWS program development.

SECTION 2: EVALUATING ACCESS POINTS

Evaluating access points is a critical and challenging component of implementing an effective AWS program that minimizes operational impact and increases buy-in from the airport community. Airports should consider the following factors when evaluating access points:

- **Data collection and assessment:** Data collected from the airport's access control system can be used to evaluate aviation worker traffic through potential AWS points. This data can include the number of transactions by time, day, season, and other trend information essential to determining the optimal locations for AWS. This data can also be beneficial for demonstrating to stakeholders why some access points could be restricted or closed.
- **Screening location:** Evaluate space at each qualified access point to determine the optimal location of AWS activities (i.e., whether AWS will occur prior to entry to the Secured/Sterile Area, immediately after entry, or within the Secured or Sterile Area). The impact on tenant space is an important consideration.
- **Footprint considerations:** The design of the screening point needs to fit the available space. Consider the size and layout of equipment and the flow of workers.
- **Required security measures:** Determine the level of security screening procedures required and ensure suitability with those selected access points.
- **Closure/restriction:** Some door locations might not be suitable for screening due to space constraints, location near tenant spaces, and traffic flow concerns.

Considerations for selecting access points:

- **Closing access points:** This might cause inconvenience and require alternative routes for workers and contingency plans for oversized bags and other operational factors. However, closing access points might also facilitate the airport's control over the screening process.
- **New processes:** Implementing new screening procedures requires clear communication and training for workers.
- **Future challenges:** Consider how screening can be expanded or integrated with other systems to meet future operational needs, such as full AWS.
- **Stakeholders buy-in:** Gaining support from stakeholders in the selection of access points to conduct AWS and the closure of access points that are deemed unnecessary will require education, collaboration, extensive communication, and possibly negotiation. The use of data on access transactions to support decision making is strongly recommended.
- **Emergency exits:** Alternative exits may be required for emergencies. Balance security with emergency access needs.
- **Exemptions:** Populations as defined by the NA and any populations granted local TSA approval, as applicable.

Space, infrastructure, and least operational impact for the various stakeholders may be the primary factors when selecting AWS locations for many airport operators.

During the airport discussion groups, many airport operators noted that space was their deciding factor on where to have screening take place, and that the area before the access point was predominately preferred since this is where the most space was available. In addition, having the screening occur before the access point can provide the opportunity to resolve alarms or issues prior to entry. However

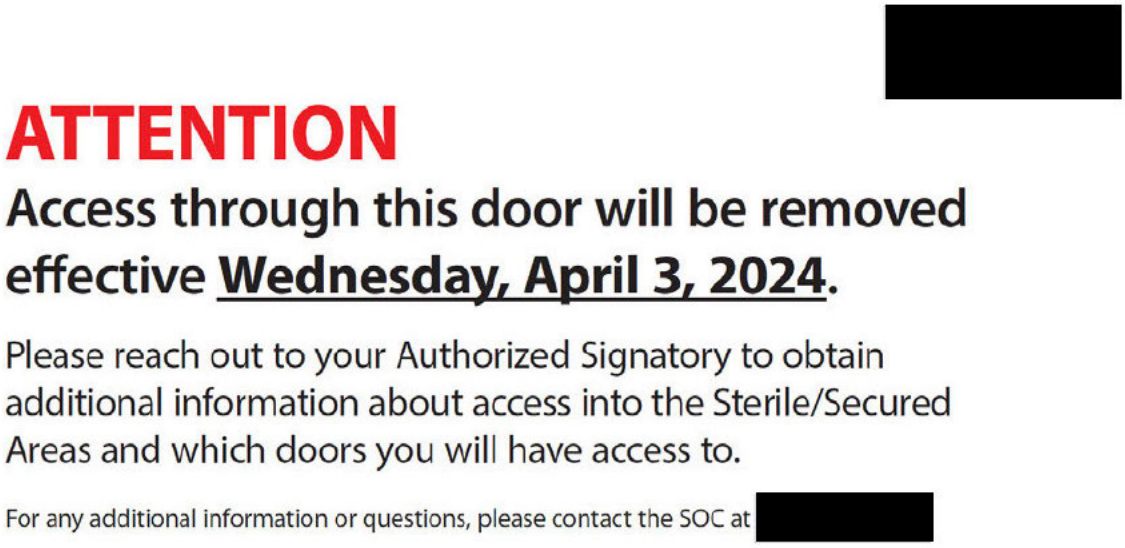
conducting AWS before the access point must be approved by the local TSA office. Assistant FSDs for Regulatory Inspections and Screening will be useful resources in this process.

An access control card reader should be placed at the screening area entry point to verify the worker's badge prior to screening.

2.1 Coordination with Stakeholders

Strong coordination and collaboration with airport stakeholders, TSA, airlines, ground handlers, concessions, and security contractors regarding the reduction or use of access points for AWS is critical. Stakeholders will be the most impacted by the implementation of AWS, and altering the access points they use to gain entry to the Secured/Sterile Areas will further impact their operations, including employee arrival, departure, clocking in for work, and performance of duties that require moving between the public space and the Secured or Sterile Area. Once access point have been reviewed, it is recommended that the airport post notices at the doors scheduled to be closed, as shown in Figure 2-1.

Figure 2-1. Door Closure Notice



Coordination with local TSA regarding access points is highly recommended. This includes meeting and coordinating with the local TSA officials on access points that will be closed or restricted and those that will be factored into the AWS program.

Airport law enforcement departments that assist with alarm resolution will need to know which access points are being used for AWS, which have been closed, and which are used for emergency access.

Airport operators should walk the terminals with stakeholders, law enforcement, and TSA to evaluate and gain buy-in for the portals selected for the AWS program or for restricted access.

SECTION 3: STAFFING MODELS

Airport operators face a complex decision when choosing a staffing model to perform AWS in accordance with the governing NA. This decision is a culmination of financial, operational, legal, labor market, and other factors, which differ based on the airport's governance, organizational culture, and region. The following staffing models are discussed in this section:

1. **Direct Airport Employees:** The airport directly hires and manages the screening staff.
2. **Security Contractors:** The airport hires a security company that provides and supervises the screening staff.
3. **Hybrid:** The airport uses a combination of direct airport employees and security contractors.
4. **Airport Law Enforcement:** Airport law enforcement provides the screening staff and supervision.

To determine the most suitable staffing model, airport operators should conduct a thorough analysis of the requirements of AWS and consider the following factors:

- **Operational:** Screening experience and expertise of personnel, capacity to handle the workload, and space needed to conduct screening operations.
- **Financial:** Cost of salaries, benefits, training, equipment, supplies, and operations and maintenance contracts to support each model.
- **Technology:** Use of screening equipment and technology with the chosen model.
- **Logistical:** Ease of implementation and integration of the screening program.
- **Regional Workforce Conditions:** Availability of local workforce.
- **Legal:** Compliance with governing security and operational regulations and local laws, and protecting the airport from liability concerns.
- **Labor Relations:** Collective bargaining agreements may dictate the staffing model chosen by the airport.
- **Management:** Oversight, assignment of responsibilities, and assurance of performance.
- **Training:** Ensuring adequate training and knowledge retention for all screening staff, as well as identifying deficiencies to provide remedial actions.

Each model offers distinct advantages and disadvantages that need to be assessed to select the model that is best aligned with the airport's governance, culture, operations, resourcing, market conditions, funding, and legal and risk postures.

3.1 Direct Airport Employee Staffing Model

Airport operators that choose to staff AWS checkpoints with direct airport employees will need to ensure recruitment and retention are in place to support the needs of AWS.

Airport operators with existing employees conducting similar work, such as access control responsibilities and inspections, may amend the employee responsibilities as needed or hire additional staff to perform this function. This will require revising existing job descriptions or drafting new job descriptions to encompass AWS responsibilities, as well as providing appropriate training.

Airports under the management of their city, county, or state would likely determine that using airport employees would come at a higher cost, given the pay rates, associated employee benefits, and training.

However, although this staffing model may be more expensive generally, airports interviewed reported efficiency gains and other benefits afforded by the flexibility to redeploy these workers to perform different functions (e.g., security, operations, or other duties during periods of limited screening operations). The staffing costs for direct employees will also be fixed, unlike contractor costs that may fluctuate based on availability, competition, and operating hours.

Using directly employed staff for AWS requires careful analysis of costs, benefits, legal concerns, and workload management. However, with proper planning and implementation, it can provide increased control and flexibility for airports.

Table 3-1 outlines some of the advantages and disadvantages associated with this staffing model.

Table 3-1. Direct Airport Employee Staffing Model Advantages and Disadvantages

Advantages	Disadvantages
• Efficient deployment • Flexibility to cross-utilize job roles • Career development opportunities • Commitment to the organization • Increase motivation and job satisfaction • Greater control over job performance • Direct management oversight • Drive assurance activities • Fixed costs	• Management oversight required • Higher costs (salary and benefits) • Approval needed to increase staff • Lengthy hiring process • Labor union engagement • Risks and liability • Recruitment and retention of staff • Training needs (time, money, resources)

3.2 Security Contractor Staffing Model

Security contractors currently provide US airports with a variety of security services to meet the complex security needs of the aviation industry. Contractor screening expertise and high performance standards are recognized by the TSA through their Screening Partnership Program (SPP), which contracts security screening services at commercial airports to qualified private companies.[2] These companies manage and implement security screening operations under federal oversight and must comply with all TSA security screening procedures using federal equipment.

With many security contractors being trained in stadium-style searches (versus general guard services), the contractor option has proven to be viable for many airports as they implement AWS. The differences in desired competencies and skills between general guard service contractors and those with security screening expertise is vast and must be assessed during any contractor selection process. Airports should consider security contractors who can deliver high-level screener capability, both in expertise and the ability to maintain staffing levels.

Airports endorsed contract security companies with extensive security screening experience at other airports, as their proficiency level was high, management oversight was effective, and the company was able to share best practices from the other airports where they conduct AWS. The sharing of best practices between airports is an advantage over direct airport employee screening. Airports should also

[2] https://www.tsa.gov/for-industry/screening-partnerships.

consider engaging security contractors with a strong international presence in countries with existing AWS programs.

Airport operators utilizing contract security staff generally noted that there is potentially less risk associated with hiring contract staff versus direct airport personnel as the primary liability for screening would typically be incurred by the contractor. Benefits also included staff who are already trained in security services, and the flexibility to employ personnel without full-time equivalent (FTE) requirements.

Airport operators also noted that, while costs for contracting screening services may seem high compared to using direct airport personnel, the overall costs would generally be lower than the fully loaded salary and benefits package associated with using direct personnel. Ease of quickly deploying workers to conduct AWS, prior screening experience, and less management overhead required by the airport were also primary reasons for using contractors rather than direct airport staff. Additionally, airport operators can delegate responsibilities to the security contractor for training, deployment of roles, development of Post Orders, and reporting.

Specific training and testing on the requirements in the NA and the airport's procedures for compliance will be required. Several security contractors deploy proprietary apps to deliver training and knowledge checks that test retention of critical information, identify proficiency levels, and ensure compliance.

Performance outcomes are a key deliverable for a security contractor, and the airport will need to set expectations and monitor performance to ensure compliance with screening protocols, efficient recordkeeping, and reporting. Reporting needs to be accurate and timely to comply with the AWS recordkeeping obligations prescribed in the NA. More information can be found in Section 8: Recordkeeping and Reporting.

A key factor for consideration in engaging a security contractor is the number of operational hours of AWS at an airport, as determined by the Screening Requirements Calculator. Deploying contractors for a few hours per day is not sustainable, profitable, or attractive for a contractor to commit and deploy the required resources. If the number and schedule of AWS hours does not meet market conditions, airport operators may find it challenging to engage and retain a security contractor. Airport operators already employing a security contractor may be able to modify or change the contract to incorporate the additional requirements for AWS.

Several airports reported retention and job satisfaction issues arising from the low number of AWS operational hours and an AWS deployment schedule that varied drastically throughout the day/night. One airport that engaged a security contractor successfully mitigated these issues by employing the security contractor to conduct AWS hours at a level that exceeded TSA requirements. This approach ensured that the airport was able to hire and retain a proficient, experienced security contractor, which was necessary to implement their AWS program. Although this modification resulted in extra expense, it contributed to an effective and well-trained workforce, provided an increased level of AWS activity, and enhanced visibility, which can increase aviation workers' expectation of being screened.

Another notable consideration is contractor availability. In some regions of the country, there is a significant shortage of available contract security workforce.

Table 3-2 outlines some of the advantages and disadvantages associated with this staffing model.

Table 3-2. Security Contractor Staffing Model Advantages and Disadvantages

Advantages	Disadvantages
• Screening capabilities and experience • Faster recruitment, deployment, and implementation • Trained workforce • Flexibility without FTE obligations • Delegate responsibilities (Post Orders) • Shared liability or primary party (contractor as the primary) • Lower costs (varies by airport and market conditions in the region) • Able to share AWS screening best practices and solutions from other airports • Some contractors employ proprietary apps for training and knowledge checks of their staff • Familiarity with drafting Post Orders • Avoid human resources/personnel issues associated with direct staff	• Higher costs* (*depending on contractor availability, region, airport size, and operational AWS hours*) • Subject to continuous price increases by the contractor • Less control and flexibility • Scheduling – cyclical downtimes • Job performance, satisfaction, and attendance • Staffing shortages and turnover exacerbated by the contract personnel competing for other airport contract security work • Dependencies for reporting • Less oversight

3.3 Hybrid Staffing Model

A hybrid model uses a combination of direct airport employees and security contractor personnel. Using this model, airport operators can achieve a balance between the two options and may reap the benefits of both staffing models. Hybrid staffing model examples include:

- **Airport security management:** Airport employees oversee screening procedures conducted by security contractor personnel, which allows for airport operators to maintain oversight and control of AWS operations while leveraging contractor expertise.
- **Phased transition:** Airports can gradually shift from a contractor-based model to a direct employee model by using security contractors during the onboarding process for new staff.

Additional considerations include:

- Clear communication and collaboration between direct employees and contractors is paramount for an effective workflow and consistent security measures.
- Finding the right balance between direct and contracted workforce can optimize costs while maintaining security standards.
- Both direct airport employees and contract personnel must receive comprehensive training on screening procedures, regulatory responsibilities, and airport security protocols.

The hybrid model can offer a strategic approach to AWS. By carefully considering the benefits and potential challenges, airport operators can deliver a screening workforce that optimizes security, efficiency, and cost-effectiveness.

Table 3-3 outlines some of the advantages and disadvantages associated with this staffing model.

Table 3-3. Hybrid Staffing Model Advantages and Disadvantages

Advantages	Disadvantages
• Leverage the strengths of direct airport and security contractor models • Adjust staffing based on security needs and budget constraints • Security contractors offer expertise in performing security functions • Readily available and trained staff to support direct airport employees • Opportunity for direct employees to develop in-depth knowledge • Security contractors can serve as the interim security personnel while new direct employees are hired and trained • Airports can maintain effective oversight and control by assigning direct employees to manage the security contractor workforce • Airports can control staffing levels • Airports develop or delegate the drafting of procedures and can retain approval authority • Shared liability	• Higher costs • Subject to continuous price increases by the security contractor • Dependencies on security contractor for operations and reporting • Job performance, satisfaction, attendance • Recruitment • Training (time, money, resources)

3.4 Airport Law Enforcement Staffing Model

One airport involved in the airport discussion groups assigns responsibility to the airport's law enforcement department to manage and operate their AWS program. Similar to the direct airport employee staffing model (see Section 3.1), airport law enforcement utilizes existing employees, recruits and trains additional personnel, and operates the program. This airport's law enforcement department employs both non-sworn and sworn law enforcement officers to operate AWS. The non-sworn members are the primary screeners, and they are supervised by a sworn law enforcement officer.

A notable advantage with this model is the ability for sworn law enforcement officers to use their legal authority to streamline incident response and alarm resolution. However, this model will not be readily available for all airport operators, given the reliance on their local law enforcement agency, which may not have the capability or desire to manage and operate AWS.

Table 3-4 outlines some of the advantages and disadvantages associated with this staffing model.

Table 3-4. Airport Law Enforcement Staffing Model Advantages and Disadvantages

Advantages	Disadvantages
• Efficient deployment • Officers bring their skills and knowledge to the screening process • Use their legal authority for response and alarm resolution • Efficient use of personnel while maintaining a strong oversight structure	• Dependencies for operations and reporting • Less control for airport operator • Training (time, money, resources) • Not a readily available model

3.5 Collaborating with Airport Law Enforcement

Airport operators should collaborate with their local law enforcement when developing, implementing, and operating their AWS program. Airport law enforcement have designated responsibilities in 49 CFR § 1542, and their knowledge of the airport, experience responding to security incidents, and knowledge of relevant laws, regulations, and procedures can be invaluable for a successful AWS program implementation.

Airport operators have expressed the value of educating airport law enforcement on the requirements of the NA and ASP, and bringing the officers into the process in the early stages of establishing an AWS program, developing SOPs, coordination of information sharing. It is important that airport law enforcement understand the staffing model and the potential impact on their calls for service in support of AWS at the airport. Officers may be called to respond to an incident during the screening process (e.g., refusal by an employee to submit to screening, discovery of a prohibited item, or assistance with alarm resolution).

Early involvement fosters open communication and collaboration between airport security and law enforcement to support the understanding of roles and responsibilities. Engaging with each other from the outset, airport security, operations, and police can develop a response plan and build a more efficient and effective AWS program.

3.6 Training

While TSA does not describe specific procedures or training requirements, the airport operator must ensure that AWS personnel are trained on all security procedures that they are responsible for performing in accordance with the ASP and NA. Consequently, airport operators will need to establish airport-specific protocols, procedures, and training, or delegate these functions to their contractors, while maintaining oversight and quality assurance to comply with the NA and achieve an effective security outcome. Airports must ensure that the training provided to AWS personnel, whether direct employees or contract security personnel, encompasses all measures, procedures, and protocols they are accountable for performing, including the operation and maintenance of screening equipment.

Airport operators need to carefully consider their training needs and resources, whether they train their own employees or use contractors. Notably, consistency in training is an important consideration to ensure that all personnel conducting AWS are performing with similar standards.

DIRECT AIRPORT EMPLOYEE CONSIDERATIONS

Airports utilizing direct airport employees should consider the following elements:

- **Identifying training needs:** Determine the type of media, equipment, facilities, and costs involved.
- **Assessing skills gaps:** Identify disparities between what skills employees possess and the skills that are needed to conduct AWS.
- **Ensuring compliance and training effectiveness:** Conduct compliance monitoring to validate employee understanding and identify critical knowledge gaps. Auditing of the screening process, screener performance, and mandatory records/data collection can be accomplished by the airport or the security contractor through observation, CCTV, document review, portable devices and apps used during the screening process, and other methods. Mitigation actions may include recurrent training, on-the-spot training, or providing reference and training materials to ensure relevant knowledge transfer, avoid knowledge gaps, and identify areas of improvement.

- **Expertise and planning:** Engage suitably qualified training experts to develop and deliver consistent and comprehensive training programs.
- **Program development:** Align training with internal and external standards and equipment specifications.
- **Training schedule:** Consider the training schedules for existing and new personnel.
- **Train-the-trainer:** Determine if instructors are needed to train airport staff.

Airports that conduct in-house AWS training can benefit from greater control of training standards, scheduling, and delivery. However, this requires having dedicated training staff and resources, which might not be feasible for smaller airports.

SECURITY CONTRACTOR CONSIDERATIONS

A key benefit of using a security contractor is their access to in-house or specialized trainers, and potential cost effectiveness, especially for smaller airports. The challenge for airports is the loss of control over training content and delivery, as the training quality and consistency can vary depending on the contractor. Some key considerations when selecting a contractor include:

- Review the contractor's experience, training curriculum, content, instructors' qualifications, and delivery methods.
- Ensure the contractor's training programs meet the airport's requirements.
- Ensure training covers the proper use and operation of screening technology in addition to the program requirements specified in the NA.
- Require regular refresher training.

SECTION 4: SCREENING METHODS

Airports can utilize physical or technology-based screening of aviation to deter insider threat and prevent prohibited items from entering the Secured and/or Sterile Areas. This section discusses both manual and technology-based screening solutions. Airport operators should consider applying a combination of security controls.

False alarm rates, environmental conditions, space, storage of tools and supplies, mobility, and equipment maintenance need to be evaluated in the equipment selection process. In addition, when selecting screening methods, airports should consider the development of the associated SOPs.

4.1 Manual Screening

Airports with a high number of qualified access points may consider manual screening as the equipment needed is generally inexpensive and highly portable. The establishment of an AWS program using handheld metal detectors and stadium-style searches of bags and accessible property has been reported to be a practical solution for airports until the explosives detection screening equipment implementation date.

There are several online resources available to review best practice procedures for stadium-style searches. An example guide is provided by the Cybersecurity and Infrastructure Security Agency at https://www.cisa.gov/resources-tools/resources/public-venue-bag-search-procedures-guide.

4.2 Technology-Based Screening

The use of technology in the screening process can enhance threat detection and provide a higher level of assurance that prohibited items will be detected. Table 4-1 includes examples of relevant technology types.

Table 4-1. Examples of Security Screening Technologies for AWS

Security Screening Equipment	Capabilities
Body scanner	Identification of weapons, explosives, prohibited items on person
Walk-through metal detector (WTMD)	Metal detection, weapons, prohibited items on person
Handheld metal detector (HHMD)	Metal detection, weapons, prohibited items on person
X-ray	Identification of weapons, explosives, prohibited items in accessible property
Explosives trace detection (ETD)	ETD of accessible property and in some cases, on person
Randomizer	IT platform for random worker selection
ID media verification platforms	Facial recognition and random worker selection

Some airport operators that have already transitioned to full AWS have implemented screening checkpoints with WTMDs, x-ray, and ETD. However, other airport operators noted that implementation

of these types of technologies may not be practical for their needs, as they could not be easily deployed for random screening at various access points.

Airports can also consider advanced imaging technology that allows the aviation worker to simply walk through the technology without stopping or removing any items of clothing or shoes. Both fixed and mobile types of this technology are available.[3]

Safe Skies has evaluated several of these types of systems at various airports through the ASSIST program. The reports of these evaluations are available to authorized airport personnel on the Homeland Security Information Network (HSIN) or from Safe Skies by request.

TSA provides a toolkit on HSIN that includes screening equipment that may be deployed for AWS.

4.2.1 Deployment and Space Considerations

The airport operator should consider the setup, portability, commissioning, and maintenance of prospective equipment, whether it is used at mobile or fixed screening locations. Both mobile and fixed screening equipment will require protocols and procedures for calibration and daily/shift checks.

Power supply should be considered to ensure the equipment for both fixed and mobile screening locations can operate effectively without restriction. Network connectivity across the screening locations will support operations and reporting. However, some airports reported the Wi-Fi router caused interference with their high-resolution walk-through millimeter wave security screening solutions.

Airport operators who are establishing a fixed checkpoint should consider the space required, noting the size of the screening/inspection equipment, user areas, throughput areas, proximity to tenant spaces, and reconstitution areas. Another key consideration is the flooring and ceiling supports. Screening equipment can be large and heavy, so airports should consult with their engineering departments before procuring it. Airport operators should involve their engineering and planning departments early in the screening point design for different layout options, infrastructure, and technology requirements.

Airports that have established fixed screening stations for concessions and goods may consider utilizing these locations for the screening of aviation workers, depending on space, circulation, foot traffic, and other contingencies.

4.2.2 Closed-Circuit Television

Using CCTV cameras to monitor AWS should be strongly considered. CCTV footage serves as a documented record of the screening process, which can aid in investigations of discrepancies or security incidents and reduce the risks associated with complaints or claims.

The benefits of incorporating CCTV into both mobile and fixed screening include increased transparency, stronger accountability, deterrence of potential misconduct, ability to forensically monitor activity and performance, and the availability of evidence for investigations and claims.

[3] Safe Skies has evaluated several of these types of systems at various airports through the ASSIST program. The reports of these evaluations are available to authorized airport personnel on the Homeland Security Information Network (HSIN) or from Safe Skies by request.

Careful camera placement is crucial to capture the entire screening process while still respecting privacy during bag searches. Airports may consider using a footprint floor marking to identify the location for the worker to be screened that will ensure the process is captured by CCTV.

SECTION 5: ESTABLISHING STANDARD OPERATING PROCEDURES

Establishing a strong AWS program requires careful consideration of several key elements. AWS procedures should be clear, concise, lawful, practical, and easily understood. These SOPs will provide the basis for training and will be a critical piece of evidence in a legal claim or a complaint. Unlike TSA's standardized passenger security screening procedures, AWS procedures and alarm resolution protocols can vary significantly between airports.

Early engagement with key stakeholders is paramount to developing SOPs. Airport operators should consult with their security, operations, legal, and risk management departments; security contractor; TSA; and law enforcement. This will help ensure roles and responsibilities are agreed upon and understood and support the development of the AWS SOPs. Engaging with TSA may be valuable, given their subject-matter expertise and insights.

Airports can also leverage existing procedures developed to comply with the TSA Insider Threat Information Circular and Security Directive that instructed airports to conduct random Secured and Sterile Area inspections of aviation workers and their property.[4]

Note that airport operators must amend their ASP and applicable EAAs to address the procedures in the NA. SOPs are not required to be included in the ASP.

Example SOPs and Post Orders are available to ASCs by request to Jessica.Grizzle@sskies.org.

5.1 Responsibilities

The development of SOPs and/or Post Orders is a critical element to design, establish, and operate an AWS program. Airports can develop these documents within their security department or they can outsource to their chosen security contractor.

Airport operators may consider developing their own SOPs if they are conducting the AWS themselves. This enables the airport operator to make necessary and timely changes to the SOP. Airports that are governed by city, local, or state government agencies should assess the timeline needed to develop, review, and approve new airport employee procedures.

If the airport is using a security contractor, SOP development might involve drafting an initial SOP for security contractor feedback or providing the security contractor with general guidelines to develop an SOP or Post Orders. This will provide an opportunity for the security contractor to tailor the language to align with their workforce requirements. Established security contractors may already have existing SOPs/Post Orders deployed across airports that can be amended to suit other airport operators. If an airport assigns the responsibility of SOP and/or Post Order development to a security contractor, the airport's security department can maintain control by governing the review and approval of the procedures. SOP/Post Order development is an important contract provision, and the airport should specify how this task will be performed (e.g., in concert or delegated to the security contractor with approval by the airport or other method).

[4] Information Circular-15-01E, August 30, 2018. Security Directive 1542-18-01A, December 6, 2018

Regardless of the chosen method to draft and establish the SOPs, airports must ensure they are developed to effectively apply AWS to local operating conditions and response actions, and to comply with the NA, security regulations, and the ASP.

5.2 Alarm Resolution SOP

Alarm identification, response, and resolution are important considerations in an AWS program. Airport operators should collaborate with their TSA office and law enforcement to ensure the SOPs/Post Orders align with available response actions.

A no-touch policy for screening aviation workers is common for airport operators, given the litigation risks and challenges when attempting to clear alarms (refer to Section 10: Legal Considerations). Airports with this policy must identify suitable solutions to clear a worker who cannot be cleared using the access point screening methodology. Notable solutions require the airport to enlist the support of TSA and/or local law enforcement. Airport operators could escort the worker to the TSA passenger screening checkpoint for additional screening. Where this is not feasible, the airport may opt to utilize local law enforcement to assist with clearing alarms. Airport operators should consider the use of CCTV to provide assurance of the no-touch policy and to support compliance and incident investigations or liability claims (refer to Section 4.4.2: CCTV).

Airport operators that rely on TSA or local law enforcement should also consider options to clear an alarm when the selected method is not available, such as when the TSA passenger screening checkpoint is closed and/or local law enforcement officers are not present. The contingency measure could be to temporarily suspend or confiscate the worker's ID media to restrict access privileges and entry into restricted areas.

5.3 Prohibited Items SOP

SOPs and Post Orders should include notification requirements for when a prohibited item is discovered during the screening process. Notification requirements are covered and detailed more thoroughly in Section 8, but the airport operator should ensure notification requirements are established in the SOPs and Post Orders.

The specific procedures for managing prohibited items may vary depending on the security capabilities of the airport. The airport must establish procedures for the safe confiscation, storage, and disposal of prohibited items. Additionally, the procedures could provide options for the aviation worker to return certain prohibited items to another location (e.g., landside office or private vehicle). Collaboration with local law enforcement can be crucial for investigations and response to incidents involving prohibited items.

5.4 AWS Scheduling SOP

Airports have three options for scheduling AWS:

1. **TSA Random Screening Scheduler (RSS):** This tool was designed to calculate the required screening hours and generate a random schedule.
2. **Airport-Generated Schedule:** Using the screening hour output from the TSA RSS, airports can create their own schedules, pending review and approval from the FSD. This can provide customization but may require additional effort to develop, which may not be ideal for airports lacking the resources for in-depth scheduling.

3. **Enhanced Scheduling Tool for Aviation Worker Screening:** Using the screening hour output from the TSA RSS, this tool enables airports to create efficient and adaptable AWS schedules that cater to their specific circumstances, pending review and approval from the FSD. Version 1.2 of the tool includes the ability to weight access portals based on comparative risk. Version 2.1 does not include this option.

The Enhanced Scheduling Tool for Aviation Worker Screening and its supporting documentation are available from Safe Skies by request.

The TSA's RSS offers a basic solution, while developing an airport-generated schedule provides more control, although with more effort. The PARAS 0059 Enhanced Scheduling Tool for Aviation Worker Screening could offer a balance between ease of use and customization. Choosing the best option depends on an airport's specific needs and resources, as well as compatibility and compliance with TSA regulations.

The SOP should include a section that explains the scheduling method and outlines the implementation and operational processes. These procedures should address assigning roles and responsibilities, and reporting requirements. By incorporating scheduling information effectively, the SOP will support compliance and serve as a robust guide for AWS.

5.5 Compliance and Enforcement SOP

Airport operators should ensure the compliance and enforcement section of the SOP addresses procedures to manage and report the following:

- Detection of unauthorized weapons, explosives, and/or incendiaries
- Refusal to be screened
- Circumvention of screening
- Other security violations that may occur during the AWS process

SOPs and Post Orders may also include how testing of screening personnel is conducted. Additionally, airport operators should ensure that their rules and regulations, orders, and policies provide a mechanism to enforce penalties and corrective actions for AWS program violations. If airports do not have relevant rules and regulations in place, they should consider amending existing security rules and regulations.

5.6 SOP Elements

Airport operators can use the content examples below to design effective and adaptable AWS procedures that meet their specific needs and comply with overarching security standards.

Content Examples

- General Information
- Purpose
- Definitions
- Post Staffing
- Post Required Equipment
- Contact Numbers

Content Examples
• Employee Screening Schedule • Exemptions from Screening • Operating Procedures • Opening the Post • Conducting Screening Activity • Media Verification • Equipment Type Screening (WTMD, X-Ray, HHMD, ETD, etc.) • Property Inspection • Prohibited Item Discovery • Tools of the Trade • Completing the Inspection • Closing the Post • TSA Inquiries and Testing Procedures
Appendices
• TSA Definitions • Prohibited Item List • Screening Log • Incident Report • Employee Statement

SECTION 6: PROHIBITED ITEMS

Airports can employ various approaches and strategies to define prohibited items in alignment with the airport's specific governing policies, laws, and regulations.

6.1 Developing a Prohibited Items List

When developing a prohibited items list (PIL), one place to start may be the TSA's prohibitions in the Sterile Area, which are listed on their website: https://www.tsa.gov/travel/security-screening/whatcanibring/all-list. A PIL should include descriptions of weapons, explosives, and incendiaries, like the TSA website descriptions of prohibited items. The TSA's list can be used as a template to guide development. Potential modifications include:

- Allowing tools of the trade to enter the Secured or Sterile Area with relevant local approvals and protocols, including local TSA approval, as applicable.
- Adding possession of alcohol or narcotics due to associated safety risks.

Another source for airport operators to consider is international best practices and standards. ICAO provides a general framework for countries to develop regulations on prohibited items, and has published a working paper that includes generic categories of dangerous items:[5]

Category I: Firearms, Guns, and Weapons: This includes any object capable of discharging a projectile or causing serious injury. Examples include firearms, ammunition, replica firearms, and explosives.

Category II: Explosive and Flammable Substances: This category covers materials that can readily ignite, explode, or generate dangerous fumes. Examples include fireworks, lighter fluid, gasoline, compressed gas canisters, and some camping equipment.

Category III: Chemical and Toxic Substances: This includes any chemical or toxic substance that poses a health risk to passengers and crew or could be used to create a dangerous device. Examples include bleach, corrosive materials, poisons, and some laboratory chemicals.

Category IV: Pointed/Edged Weapons and Sharp Objects: This category covers any item with a sharp point or edge that could be used to cause serious injury. Examples include knives, scissors exceeding a specific length, box cutters, axes, and ice picks.

Category V: Blunt Instruments: This category includes any object capable of inflicting serious injury through blunt force trauma. Examples include crowbars, hammers, baseball bats, and certain martial arts equipment.

Additional considerations when establishing a PIL include:

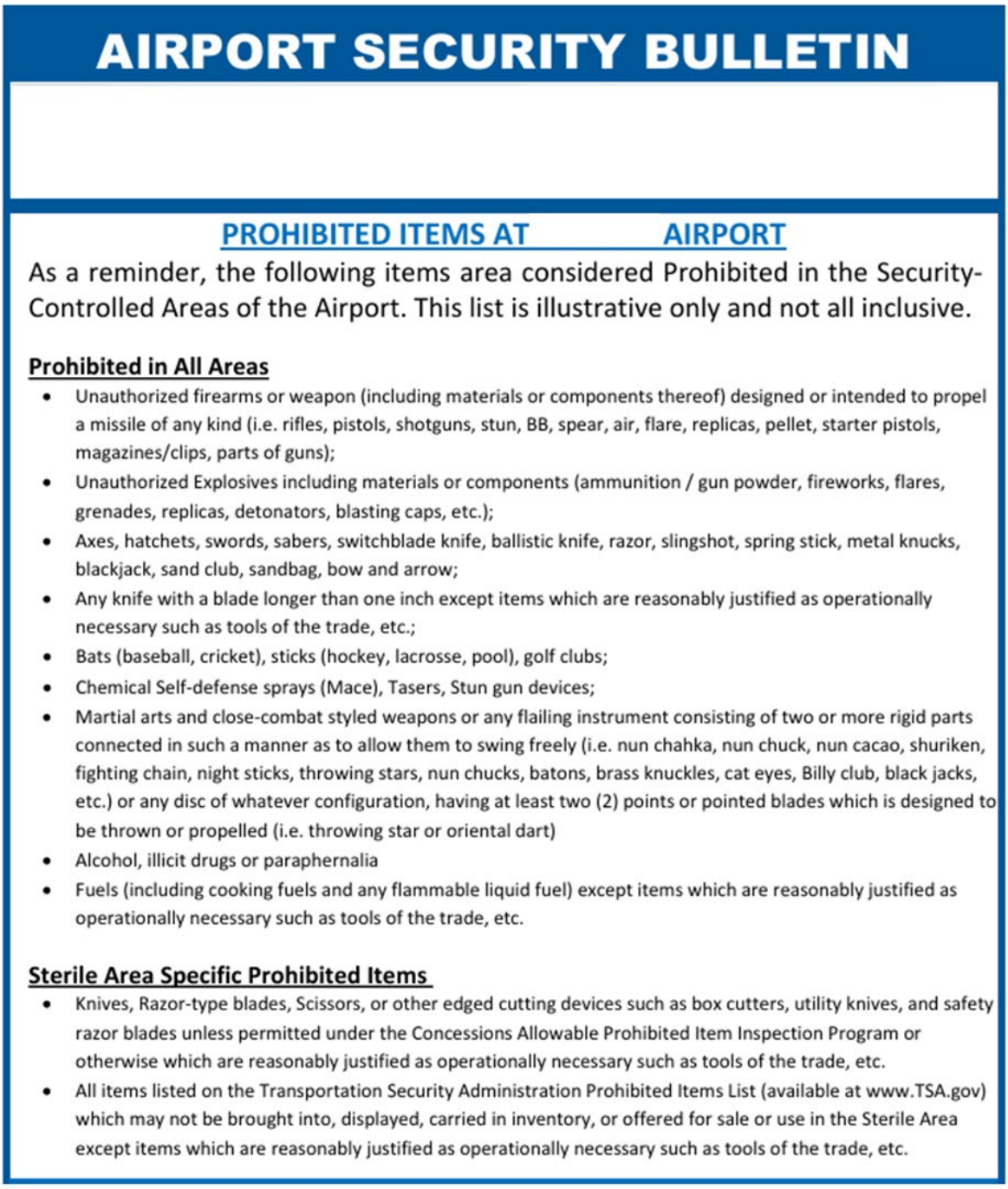
- Developing separate lists for Secured Areas and Sterile Areas. This option provides flexibility to allow items that are not suitable for Sterile Areas to be carried and lawfully used in Secured Areas.
- Adopting a hybrid list based on TSA's PIL and the airport's policies, laws, and regulations.
- Collaborating with airport tenants, TSA, and law enforcement.

[5] https://www.icao.int/safety/DangerousGoods/Working%20Group%20of%20the%20Whole/WP.50.AppA1.pdf

- Using disclaimer language stating that the PIL is not all-inclusive and that there may be other items that are prohibited, dangerous, or present a risk; the airport has discretion to restrict additional items that do not appear on the PIL.

Figure 6-1 shows an example PIL that may be displayed at strategic locations near the AWS areas.

Figure 6-1. Sample Prohibited Items List



AIRPORT SECURITY BULLETIN

PROHIBITED ITEMS AT AIRPORT

As a reminder, the following items area considered Prohibited in the Security-Controlled Areas of the Airport. This list is illustrative only and not all inclusive.

Prohibited in All Areas

- Unauthorized firearms or weapon (including materials or components thereof) designed or intended to propel a missile of any kind (i.e. rifles, pistols, shotguns, stun, BB, spear, air, flare, replicas, pellet, starter pistols, magazines/clips, parts of guns);
- Unauthorized Explosives including materials or components (ammunition / gun powder, fireworks, flares, grenades, replicas, detonators, blasting caps, etc.);
- Axes, hatchets, swords, sabers, switchblade knife, ballistic knife, razor, slingshot, spring stick, metal knucks, blackjack, sand club, sandbag, bow and arrow;
- Any knife with a blade longer than one inch except items which are reasonably justified as operationally necessary such as tools of the trade, etc.;
- Bats (baseball, cricket), sticks (hockey, lacrosse, pool), golf clubs;
- Chemical Self-defense sprays (Mace), Tasers, Stun gun devices;
- Martial arts and close-combat styled weapons or any flailing instrument consisting of two or more rigid parts connected in such a manner as to allow them to swing freely (i.e. nun chahka, nun chuck, nun cacao, shuriken, fighting chain, night sticks, throwing stars, nun chucks, batons, brass knuckles, cat eyes, Billy club, black jacks, etc.) or any disc of whatever configuration, having at least two (2) points or pointed blades which is designed to be thrown or propelled (i.e. throwing star or oriental dart)
- Alcohol, illicit drugs or paraphernalia
- Fuels (including cooking fuels and any flammable liquid fuel) except items which are reasonably justified as operationally necessary such as tools of the trade, etc.

Sterile Area Specific Prohibited Items

- Knives, Razor-type blades, Scissors, or other edged cutting devices such as box cutters, utility knives, and safety razor blades unless permitted under the Concessions Allowable Prohibited Item Inspection Program or otherwise which are reasonably justified as operationally necessary such as tools of the trade, etc.
- All items listed on the Transportation Security Administration Prohibited Items List (available at www.TSA.gov) which may not be brought into, displayed, carried in inventory, or offered for sale or use in the Sterile Area except items which are reasonably justified as operationally necessary such as tools of the trade, etc.

6.1.1 Federal Law (49 USC § 1540[b])

Federal law under 49 USC § 1540(b) provides the legal framework for TSA to enforce security measures at airports.[6] This law prohibits carrying dangerous weapons or explosives into Sterile Areas only, and does not cover Secured Areas. Airport operators should be aware of their state legislation concerning weapons and explosives in Secured Areas, as this is not covered by federal law.

6.1.2 Handling and Disposal of Prohibited Items and Weapons

Prohibited items and weapons (other than firearms) detected during AWS must be surrendered, and should be stored in a secure location until they are disposed of or are returned to the owner.

Airport operators can manage physical destruction of prohibited items or delegate this responsibility to contractors. In some instances (if appropriate), the aviation worker could return the item to their office or another location (e.g., vehicle) to prevent the item from being confiscated or destroyed. Airports can also consider using the TSA Amnesty Box or collaborating with a terminal storage tenant who could temporarily store these items for workers.

Airport operators should investigate these options, evaluate legal considerations related to confiscating property, and incorporate these decisions into their SOPs, training, and communications with airport tenants, ensuring all are informed of the airport's policy. Additionally, the discovery of unauthorized weapons, explosives, or incendiaries during AWS should be escalated in accordance with the airport's response procedures, including law enforcement involvement.

6.2 Tools of the Trade

A weapon or prohibited item *may* be considered a "tool of the trade" if the aviation worker needs the item to perform their job in a Secured or Sterile Area, and the purpose is lawful.

Tools of the trade should not be visible or accessible to the public, and must be under visual and physical control at all times by the person carrying and using the item. The person ceases to have control of the item if they allow it to be accessed or used by a person for whom it is not a tool of the trade. Aviation workers should always maintain a comprehensive register of their tools. If an authorized official requests the inventory or register, it must be produced for inspection, and it must match the tools carried by the aviation worker.

Airport operators should consider the serious implications if a tool of the trade is found unsecured in the Secured or Sterile Area. The implications could include the evacuation of the Sterile Area, aircraft delays, potential litigation in response to significant financial loss for stakeholders and customers, TSA enforcement actions, and reputational damage.

Airports with robust security rules and regulations have also developed a set of rules governing possession of prohibited items by visitors under escort in the Secured or Sterile Area. These individuals are authorized to possess tools of trade only when the following conditions are met:

a. The prohibited item is necessary for the performance of the unbadged worker's duties.
b. The authorized escort closely monitors the use of the prohibited item.
c. The prohibited item is not accessible to any passenger or unauthorized person.

[6] https://www.ecfr.gov/current/title-49/subtitle-B/chapter-XII/subchapter-C/part-1540/subpart-B?toc=1

d. The prohibited item is removed once the assigned duties are completed and the unbadged person leaves the Secured or Sterile Area.

Airports should consider additional security protocols to regulate the possession of prohibited items, such as:

- Require a written inventory of the items.
- Confirm that the item is required for the job the worker is currently performing.
- Ensure control and accountability of the item is always maintained, including securing the item when not in use or monitored by the worker when not being used.
- Violations of security procedures may subject the violator to a security citation or loss of access privileges.

6.2.1 Managing Tools of the Trade

Airport operators developing SOPs, policies, and procedures to manage tools of the trade within Secured or Sterile Areas should consider the following.

Application: This process requires aviation workers to fill out an application to request permission to bring specific tools into the Secured or Sterile Area. This could involve a dedicated online form, paper application, additional ID media form, or other designated method. The application should clearly outline responsibilities for using tools of the trade and the information needed to determine appropriate permissions, such as:

- Worker identification
- Type and description of tools needed
- Reason for needing the tools in the Secured or Sterile Area
- Estimated duration of tool use in the Secured or Sterile Area

See Appendix A for an example permit application.

Review and approval: The process for approving applications/requests should be clearly defined. Appropriately qualified staff should review each request based on predetermined criteria to ensure the tools are necessary and pose no security risk. Factors considered could include:

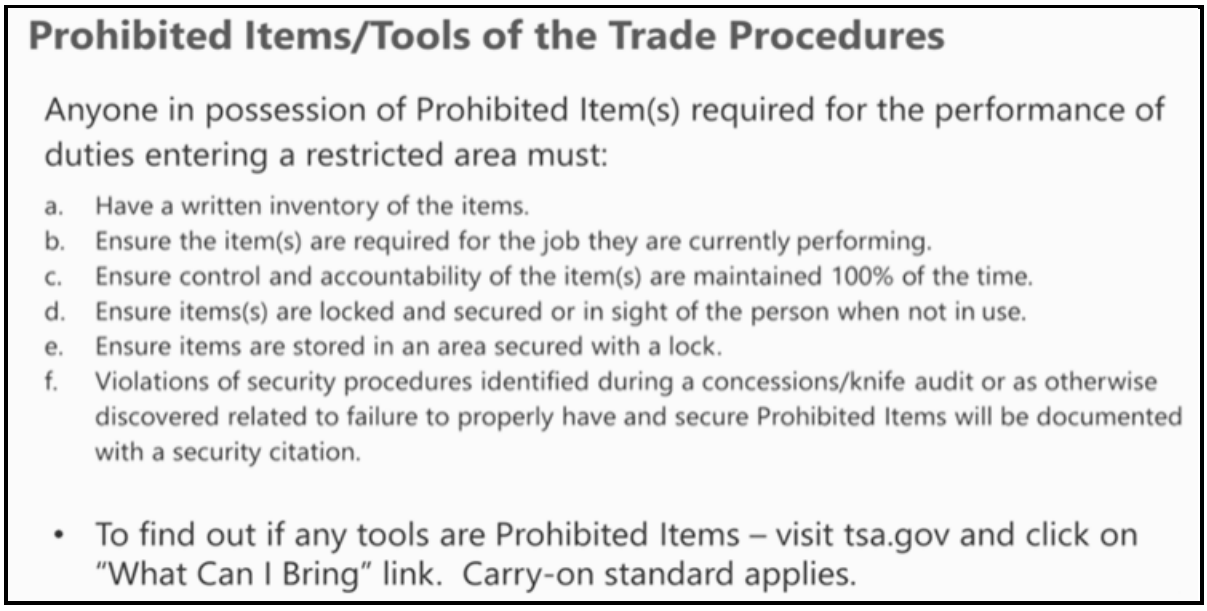
- Legitimacy of the operational purpose and work requiring the tools
- Availability of alternative, non-threatening tools
- Past security record of the applicant

Training and education: Aviation workers who are approved to carry tools of the trade should receive appropriate training to inform them of their responsibilities, including:

- Secure handling and storage procedures within the Secured or Sterile Area
- Reporting lost tools immediately
- Recognizing and preventing potential misuse of the tools
- Potential consequences if the handling requirements are breached

Providing the aviation worker with a set of instructions to read and sign (see Figure 6-2) is an effective method to confirm receipt and understanding.

Figure 6-2. Sample Instructions for Tools of Trade



Declaration forms (method of declaring what tools will be carried): The aviation worker should complete a declaration form to document the specific tools they are authorized to carry into the Secured or Sterile Area on a given day. The declaration form serves as a clear record for security personnel to validate on entry to the Secured or Sterile Areas and is carried on the aviation worker's person.

Inventory/registers (available for inspection): This process involves using a comprehensive recordkeeping system for all tools authorized for use in the Secured or Sterile Area. An accurate inventory allows for tracking tools, preventing loss or misuse, and facilitating audits.

Entry and exit requirements: These outline the specific procedures for entering and exiting the Secured or Sterile Area with approved tools, including mandatory security screening of the tools with visual inspection by security personnel and verification of tool permits or declarations.

The airport may task screening personnel with obtaining approval for tools of the trade upon employee entry into the Secured or Sterile Area. In this scenario, the screener will contact their supervisor and provide relevant information (employee name, company name, uniform description, type of prohibited item). The supervisor may notify the Security Operations Center. The judgment of the supervisor, in conjunction with airport security/operations personnel, will formulate the basis for the decision, with the airport retaining the right to make the final decision.

Compliance: The airport operator must conduct or manage appropriate compliance monitoring activities. This should include random inspections of tools carried by aviation workers, assessment of inventory records and issuance logs, testing the expertise and know-how of security personnel, and procedural review.

Tenant Responsibilities: All tenants within a Sterile Area of an airport should ensure all their tools of the trade (e.g., kitchen knives) are tethered or stored in a locked facility when not in use, and that an accurate and comprehensive tool register (Figure 6-3) is located onsite and available for compliance checks. The tenant should inspect the tools of the trade against the register prior to opening or at regular intervals, as approved by the airport operator.

Figure 6-3. Sample Tool Register

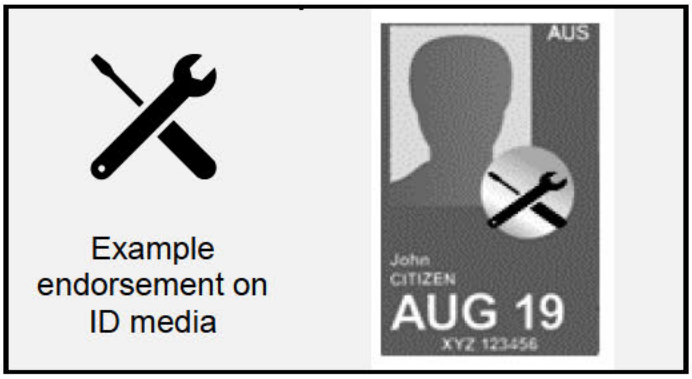
Sterile Area Tool Register

Organisation	
Date	

Date	Item Description	Item Location	Check in	Check out	Name	Signature

Identifying Authorized Individuals: Airport operators reported various options for identifying aviation workers who are authorized to carry tools of the trade into a Secured or Sterile Area. An endorsement can be added to the aviation worker's airport ID media (Figure 6-4), or a hard copy permit or license can be issued to tools of the trade holders.

Figure 6-4. Example Tools of Trade Icon



6.3 Educating the Airport Community

Airport operators must ensure that aviation workers are properly informed and educated on prohibited items and tools of the trade in Secured and Sterile Areas. Properly educating aviation workers will reduce the number of alarms during the screening process.

Airport operators should work with airline and airport tenants to ensure their employees understand the PIL, what items will be flagged at the AWS point, and what items may qualify as tools of the trade. Requirements may vary by airport, and there may be differences between the PIL utilized at TSA checkpoints and those utilized at airport-operated AWS points. These differences, if any, should be a focus of any training or briefings.

Information regarding prohibited items should be communicated across the airport community through a variety of channels, including:

- **Targeted stakeholder briefings:** One-on-one or small-group briefings can be highly effective for reaching key individuals or groups who can influence others or have a vested interest in the information. It allows for in-depth communication, addressing specific concerns, and fostering relationships.
- **Signage and awareness campaigns:** Strategically placed signs, posters, or digital displays can provide reminders and promote key messages (Figure 6-5).
- **Websites or apps:** Airport websites and apps can provide easily accessible, up-to-date information.
- **Signed Disclosure:** Notifying employees during the hiring process, and requiring a signed acknowledgment of the AWS requirements as a condition of employment, ensures all staff are aware of the regulations and procedures.
- **ID media issuance:** Integrating required language into the badge application or printing it on the back of airport badges.
- **Education at screening locations:** Screening staff can provide reminders or explanations to aviation workers during the AWS process.

Figure 6-5. Prohibited Items Poster

Source: Jacksonville International Airport

SECTION 7: COMMUNICATING WITH STAKEHOLDERS

Airports are complex facilities with a wide range of stakeholders who often have differing objectives. Airport stakeholders can be internal or external, and may include airlines, ground handlers, airport employees, tenants, passengers, government authorities, local communities, suppliers, and unions.[7]

Airport operator scheduled (e.g., committees, forums, meetings) and unscheduled (day-to-day interactions) communications are can be used to raise awareness of the AWS program, ensure consistent and proactive messaging, and ensure consistent responses to questions, all the while seeking buy-in, support, and overall compliance.

Using a planned, structured approach to communicate with stakeholders about the AWS program can help ensure that all airport stakeholders understand the program, their involvement, and the potential impacts on their movements into and out of Secured or Sterile Areas.

7.1 Leveraging Senior Executive Support

Airport operators should leverage their senior executives to support communications for AWS. Given their position and influence, they can play a crucial role in supporting the messaging and education across the airport community, including:

- **Leading by example:** Senior executives can publicly endorse AWS and the communication plan. This will show commitment from leadership and set the overall tone for the campaign.
- **Resources:** Senior executives can allocate necessary resources to ensure the communication plan is implemented effectively. This might involve the Communications/Marketing Department, funding for materials, staff training, or social media campaigns.
- **Engagement in key events:** Senior executive participation in events like committee meetings or training sessions for workers can emphasize the importance of AWS and open direct communication channels with employees.
- **Addressing concerns:** Senior executives can address major concerns regarding AWS by meeting with key stakeholders to listen to concerns and deliver consistent messaging (i.e., a "speaking tour").

While senior executives might not deliver day-to-day communication directly, their leadership and support can be critical to a successful AWS communication campaign.

7.2 Establishing a Reasonable Expectation of Screening

Airport operators must notify aviation workers possessing airport-issued ID media that they may be subject to screening for unauthorized weapons, explosives, or incendiaries; and that the aviation worker's non-compliance with the airport's AWS policies may result in further action, which could include penalties, confiscation of the individual's airport-issued ID media, and/or revocation of the individual's unescorted access authority. Figure 7-1 shows an example of such a notice.

[7] https://www.aviationpros.com/airports/blog/12388063/importance-of-airport-stakeholder-outreach

Figure 7-1. Notice to Airport Personnel of Impending AWS Program

AIRPORT COMMISSION
[redacted]

AIRPORT NOTICE

TO: Airport Commission Employees
Airlines and Aviation Support Services Teams
Retail, Food & Beverage, and Service Tenants

DATE: [redacted]

THROUGH: [redacted] *(original signed by)*
Chief Operating Officer

FROM: [redacted] *(original signed by)*
Managing Director, Safety & Security Services

SUBJECT: Aviation Worker Screening

In accordance with a TSA National Amendment (NA) on Aviation Worker Screening (AWS), [redacted] will be implementing required procedures effective Wednesday, April 3, 2024. As part of the required AWS procedures, this notice is being sent out to all Aviation Workers possessing an Airport ID Badge. Please note the following requirements:

- Aviation workers are subject to increased screening for unauthorized weapons, explosives, and incendiaries.
- Non-compliance with [redacted]'s AWS policy could result in a citation in accordance with [redacted], which could result in a suspension or revocation of your Airport ID Badge pursuant to [redacted].

For Authorized Signatories, employers, and supervisors, please immediately ensure all your [redacted] Badged employees are notified of this information and that they comply with all screening requirements.

As part of the implementation, access to the Sterile and/or Secured Area through various access points in the terminals will be removed. Authorized Signatories of each company will receive an email from Aviation Security providing a map of authorized access points through which employees may gain access into the Sterile and/or Secured Area from the Public Area. Any access point that will be removed, effective April 3, 2024, will have the sign below affixed to it.

For any questions or concerns, please contact [redacted] at [redacted].

Airport operators must post signage at access and screening points. However, signage may not be the most effective means of informing aviation workers of the screening requirements because most airports already have multiple signs posted at these locations. As such, airport operators should consider multiple means of notifying and informing aviation workers of the screening requirements, as described in the following subsections.

7.2.1 Signage

Airport operators must post signage at all access points that are public-facing doors (public-to-Sterile Area and public-to-Secured Area) portals. Airport operators can install new signage with TSA-provided language (Figure 7-2), or develop and install their own airport-specific signage (Figure 7-3). Local airport-issued signage must include the following notifications on a single sign:

- Notice of potential screening
- Unauthorized weapons, explosives, or incendiaries are not allowed in the Secured or Sterile Areas
- Refusal to undergo screening may result in penalties

Figure 7-2. TSA NA-Provided Signage/Language

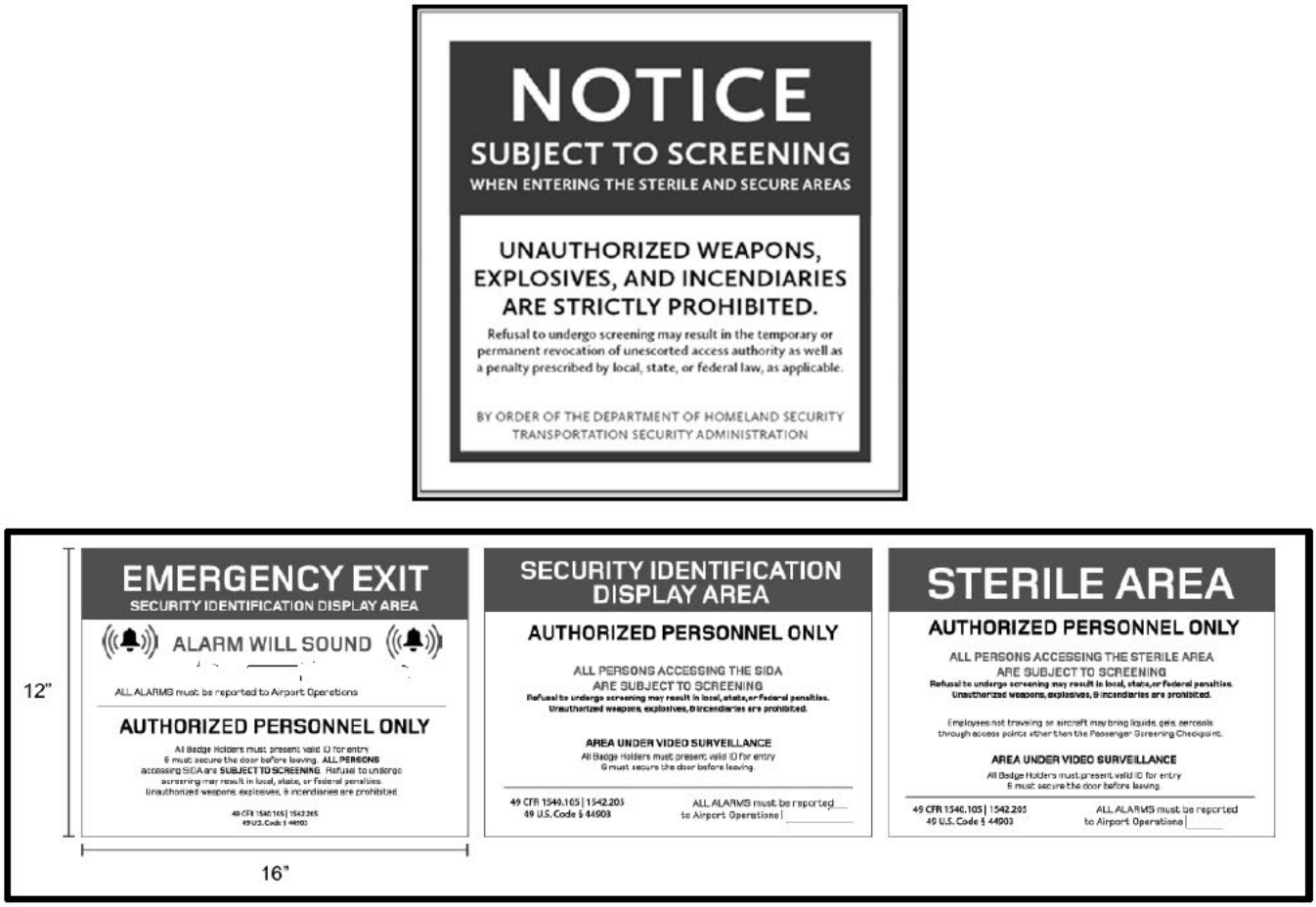
By Order of the Department of Homeland Security
Transportation Security Administration

INDIVIDUALS ENTERING
THE SECURED AREA OR
STERILE AREA
ARE SUBJECT TO SCREENING

Unauthorized weapons, explosives,
and incendiaries are prohibited.

Refusal to undergo screening may result in the temporary or permanent revocation of unescorted access authority as well as a penalty prescribed by local, state, or federal law, as applicable.

Figure 7-3. Examples of Airport-Designed Signage



Additionally, signage regarding PIL and tools of the trade can be placed strategically around the airport to serve as visual reminders of prohibited items and the screening process.

7.2.2 Publications

Publications can be an effective resource for informing aviation workers about screening procedures. An airport-published Frequently Asked Questions document could address common concerns and provide clear, concise answers. Alternatively, an Airport Security Guide could be a comprehensive resource that outlines the overall security protocols, with a dedicated section on worker screening.

7.2.3 Social Media

With the very common usage of social media to relay messages and information, airport operators may consider posting reminders to their airport community about AWS. Social media such as Facebook, Instagram, X, and the airport's web page present excellent outlets to remind all tenants and staff of the AWS requirements. These platforms can be used to remind employees (and passengers) of screening requirements and what to expect.

Some airport tenants may have internal group chats for employees to keep them apprised of schedules, and airport and flight status updates. These group chats may also be used to communicate and remind employees of the AWS requirements.

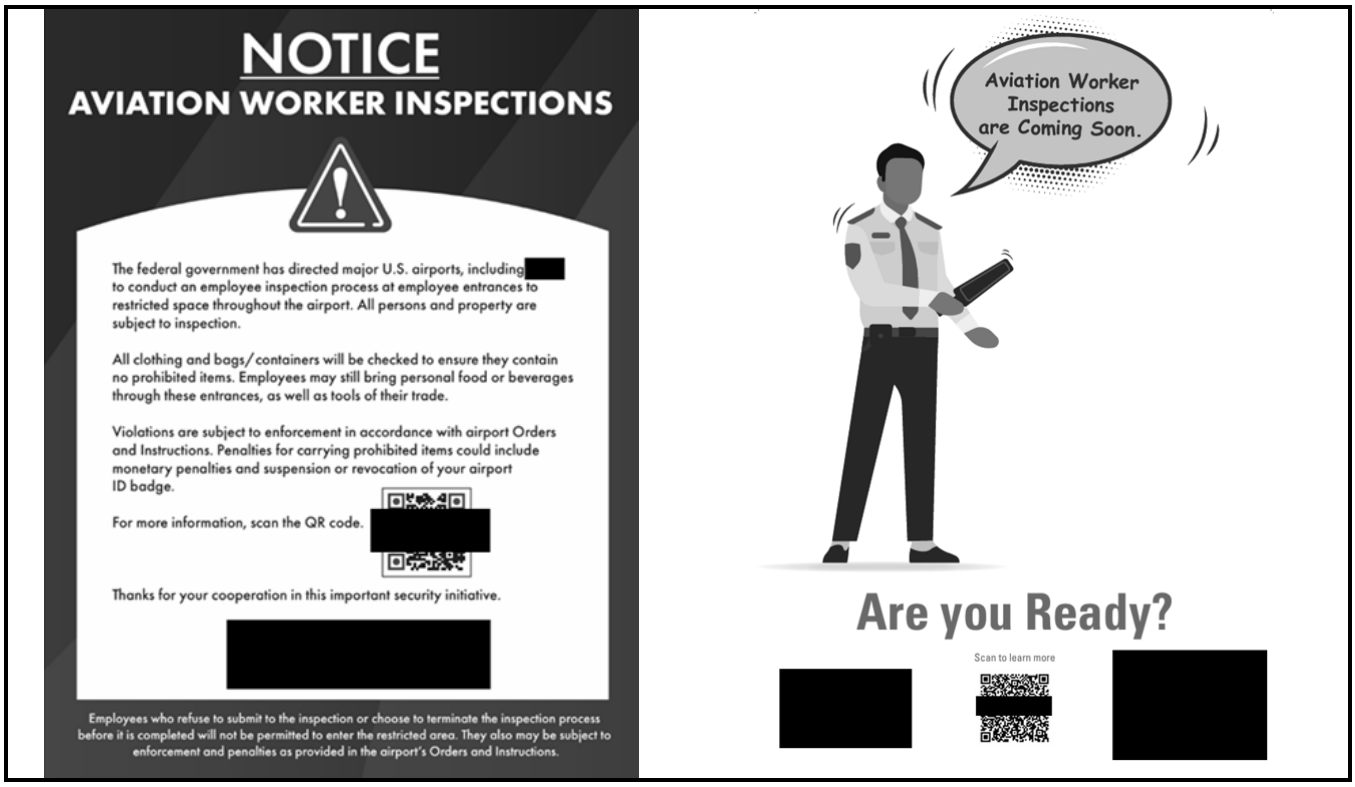
7.2.4 QR Codes

With quick response (QR) codes, airport operators can provide an interactive and user-friendly communication method to ensure all aviation workers have access to comprehensive information about the NA and screening requirements. QR codes can offer the following benefits:

- **Accessibility:** Workers can access detailed information quickly and easily using their smartphones.
- **Up-to-date information:** The webpage behind the QR code can be easily updated to reflect any changes in procedures.
- **Multilingual capability:** The webpage could offer multiple languages to cater to a diverse workforce.

Figure 7-4 illustrates an example use of QR codes in AWS communications.

Figure 7-4. Example QR Code Use



7.2.5 Airport Committees, Forums, and Meetings

Airport operators facilitate a variety of committees, forums, and meetings on a regular basis. These can be security, operational, or industry-oriented, and can be scheduled throughout the year on a monthly, quarterly, biannual, or as-needed basis. These sessions provide an effective communication channel for promoting and coordinating AWS and other airport activities, addressing stakeholder concerns, and reporting on recent and future AWS developments.

7.2.6 Airport-Issued ID Media Application

TSA has required airports to insert a "screening notice" in all SIDA ID media applications, including both electronic and paper formats. Airport operators should also consider adding this notification to the back of the ID media. The notification should include:

1. Notice of potential screening
2. Declaration that unauthorized weapons, explosives, or incendiaries are not allowed in the Secured or Sterile Areas of the airport
3. Notice that refusal to undergo screening may result in penalties

7.2.7 SIDA Training

Airport operators should consider reviewing their SIDA training process as another means of complying with the NA requirements to ensure that all aviation workers are informed of the screening requirements.

Implementing this change may take time, and may initially apply only to new ID media holders. As the ID media expire and are renewed, all ID media holders will receive the updated training that includes the new language on AWS requirements.

7.2.8 AWS Program Information Sessions

Airport operators may hold additional information sessions and collaborative training sessions with airlines and tenants, such as during their shift briefings or other training. During these information sessions, the airport operator can outline the requirements for AWS, discuss the consequences for refusing to undergo screening, and discuss the PIL and tools of the trade requirements. Airports should consider providing on-the-spot education (reminder briefings) during screening to inform aviation workers who are unaware of or challenge the requirements.

SECTION 8: RECORDKEEPING AND REPORTING

In accordance with TSA regulations, specifically 49 CFR § 1542.5 (a), recordkeeping is an important aspect of ensuring evidence of compliance with the NA.

Airport operators will now have additional recordkeeping requirements to meet the NA. Airport operators should ensure the NA record retention requirements are understood across the airport offices, divisions, or security departments. This ensures ready access, consistency with other records to be made available to TSA during inspections, and a single repository of mandated records.

Airport operators must maintain records and report AWS program information to TSA. Airport operators must transmit the data in a timeframe and manner agreed upon by the FSD or designee. These reporting requirements may pose challenges for airport operators that operate more than one airport or that have multiple FSDs. To maintain consistency, it is recommended that airport operators coordinate with their FSDs to establish a common reporting approach.

Airport operators are using internally developed or commercially available applications (apps) to support reporting requirements. These platforms allow airport operators to perform specific tasks on a mobile or desktop device, and can deliver efficiency and accuracy in recordkeeping, reduce paperwork, assist with compliance operational requirements, and provide a communication channel for collaboration among airport staff. During the airport discussion groups, several airport operators reported the use of the *AeroSimple* app.

Airports should ensure that data privacy concerns are appropriately managed and that workers are informed of how the airport will collect, store, and secure data to ensure privacy compliance.

SECTION 9: COST CONSIDERATIONS

The NA that mandates AWS is unfunded. Therefore, airports must find the necessary funds within their existing budgets, which can be a major challenge, especially considering the substantial costs involved. The earlier in the planning process the budget and financial aspects of AWS are considered, the better the airport operator will be positioned in determining how to fund the AWS program.

Careful financial analysis of the operational and capital costs of a range of screening solutions should be conducted before a final decision is made on whether to utilize a contract or direct employee screening workforce, what type(s) of screening technology will be implemented, and whether the screening locations will be mobile or fixed.

With the limited timeline for implementation of the NA, airport operators must accelerate plans and budget required to establish AWS. These accelerated plans have required some airport operators to work with their cities, counties, states, and the different authorities that oversee or manage airport operations. With some budget planning cycles being years 'out,' airport operators have had to seek additional funds to finance the screening operations to meet the NA requirements.

DIRECT COSTS

Airport operators will need to budget and fund the functions to establish and operate AWS. Airport operators have noted that the costs for AWS can be significant, depending on the size of the airport, the number of screening locations, the screening equipment used, and the screening equipment needed for future operations. Direct costs (immediate expenses) include:

- **Screening equipment:** X-ray machines, metal detectors, etc.
- **Personnel:** Hiring, training, and staffing
- **Consumables:** Supplies used for screening operations
- **Infrastructure:** Building or modifying access points
- **Security technology:** Installing additional CCTV (may help reduce insurance premiums [see Section 10.1])

Airport operators should note that purchase price is only one part of the cost of screening equipment. In some cases, a system based on low-cost equipment could prove more expensive over the operational life of high-cost equipment because of the differences in operating costs.

INDIRECT COSTS

Indirect costs for airport operators should be dependent on the size and scope of the screening operation, the size of the airport, and the number of personnel employed to conduct the screening/inspection operation. Indirect costs associated with AWS include:

- **Insurance:** Premiums might increase due to screening
- **Equipment maintenance:** Maintaining screening equipment requires contracts
- **Employee expenses:** If using airport employees, consider benefits, uniforms, and overhead

CAPITAL BUDGET EXPENDITURE

For airports that need to construct new screening checkpoints/stations, the capital needed for construction will be significant in the first and second years of the project. Once the screening checkpoints are built and implemented, the capital expenditures can be depreciated. Thereafter, normal recurring operational expenses will be incurred.

Recent Information Circulars and Security Directives from TSA have ensured that airport operators reduce access control points or implement further studies to operationally reduce the access points to a minimum at their airports. By reducing access points to an operational minimum, airport operators can focus resources on a smaller number of access control points, and therefore reduce their AWS costs.

OPERATIONAL BUDGET EXPENDITURE

Operational expenditures include recruitment, training, and deployment of either airport employees or contractors who will conduct the NA screening requirements. Insurance, maintenance contracts, and consumables will all be considered operational expenditures. These will also be recurring expenses that an airport operator must budget for future years.

SECTION 10: LEGAL CONSIDERATIONS

The screening of aviation workers raises several legal questions and concerns for airport operators. Several US Senators made public and official representations to the US Government and TSA to express their concerns and request an amendment of the NA to delay, revote, or apply more responsibility to the TSA. The American Association of Airport Executives (AAAE) and Airports Council International – North America (ACI-NA) jointly opposed the NA and drafted letters to Congress signed by each association.

AAAE stated:

> The National Amendment places an undue burden on airport operators to assume screening responsibilities that have previously been the exclusive domain of TSA in an unreasonable and arbitrary timeline without conducting a thorough cost-benefit analysis or risk assessment to justify the change. TSA should be responsible for screening people and their property, including employees, not airports.
>
> …Given the continued concerns expressed by the airport community and key committees in Congress, we ask you to rescind the National Amendment. Short of rescinding the amendment, we ask you to delay its implementation by not less than one year for the reasons outlined in the letter and to ensure that aviation worker screening can be conducted by the proper entity in the most effective and cost-efficient manner. [8]

ACI-NA stated:

> [M]andate effectively imposes upon airports significant new liability risks, including potential liability from federal and state constitutional claims arising out of administrative searches, and potentially catastrophic liability arising out of an airport's inability to detect prohibited items that are later used for a criminal or terrorist act. [9]

To comply with the implementation of the NA, a comprehensive legal review with risk identification, risk mitigation, planning, and strategies to confirm and address the potential risks and challenges is recommended. This review process should ensure all local, municipal, and state laws regarding establishing an AWS program are understood and applied.

A key point of contention is the unclear division of responsibility between airports and TSA. If weapons, explosives, incendiaries, or prohibited items are missed during screening, it is uncertain who bears the legal burden, especially for airports exceeding TSA requirements. The NA provides no guidance on handling illegal substances discovered during screening, or what to do if those substances are legal under local laws. To address this gap, airports should collaborate with their local law enforcement agency to establish clear response and reporting procedures.

The DHS Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act) "provides important legal liability protections for providers of Qualified Anti-Terrorism Technologies – whether they are products or services."[10] Airport operators can use this legislation as a primary requirement when considering engaging security contractors to deliver AWS.

---

[8] https://aaae.org/lastest-from-washington/federal_80923
[9] https://airportscouncil.org/wp-content/uploads/2023/08/ACI-NA-USPC-Position-on-TSA-Aviation-Worker-Screening-Mandate.pdf
[10] https://app.safetyact.gov/lit/h/p

10.1 Mitigating Liabilities

Airport operators should discuss liability concerns with their legal counsel, state, and local law enforcement officials. And if using a contract security company, airports should ensure their AWS policies and procedures are aligned with the ones used by the contractor to guarantee a shared liability and avoid any liability gaps.

The following strategies to reduce liability should be considered:

- **"No-touch" screening:** Minimizing physical contact during screening reduces the potential for claims of excessive force or inappropriate touching.
- **Gender-specific screening:** Having screeners of both sexes available for physical searches.
- **Camera coverage:** Fixed and mobile CCTV, and body cameras for transparency and evidentiary support.
- **Alarm resolution:** Protocols established in collaboration with local law enforcement and TSA to ensure efficient and legally compliant resolution of alarms triggered during screening.
- **Screener training:** Training programs for screeners must include thorough coverage of legal aspects and limitations of their role.
- **Executive actions:** Airport leadership should take proactive steps within their authority to address potential risks associated with AWS (e.g., ensure legal policies are created, ensure airport personnel are advised of changes).
- **Risk management:** Conducting thorough risk assessments and developing comprehensive mitigation plans to proactively address potential legal issues.
- **Contractor engagement:** For airports utilizing contractors, clear communication and collaboration are essential. Contractors need to be aware of the specific screening requirements and have established SOP/Post Order procedures for handling situations that could lead to legal issues.
- **Optimizing screening equipment:** Utilizing security screening equipment enhances effectiveness and minimizes physical contact.
- **Private screening areas:** Providing private areas for screening and alarm resolution can further mitigate concerns about privacy violations.
- **Quality Assurance:** Engage the services of a third-party auditing contractor.

10.2 Refusals by Aviation Workers

Airport operators should consider the actions and procedures for if an aviation worker refuses to submit to AWS or to have an alarm resolved to the screener's satisfaction. Some airports have incorporated into their access badge policy and procedures that if an employee in possession of an airport identification and access badge does not follow or adhere to the ASP's provisions, the airport can revoke access for that individual. Airports may also consider whether AWS is covered under existing polices used to ensure compliance with 49 CFR § 1540.105, which holds that employees seeking access to Sterile Areas or SIDA must comply with all access control systems and measures.

Because screening may be a new phenomenon for many aviation workers, the requirements for AWS should be stressed to the affected worker populations. Additionally, the education of the airport community (as outlined in Section 7) is vital to the successful implementation of AWS. Equal to the program's success is that the aviation workforce understands that all personnel who work within

Secured or Sterile Areas are subject to search and are aware of the items that are not allowed in the Sterile and Secured Areas.

With AWS being new to many airport operators and aviation workers at their airports, many scenarios may present themselves where the airport community, management, and law enforcement will need to come together to ensure that issues are resolved, procedures are adjusted accordingly, and education and communication continue for all aviation workers.

10.3 Insurance Policies

Airport operators noted that with legal liabilities for the screening of aviation workers, liability insurance coverage would need to be reviewed. Some airport operators also noted a significant increase in their overall insurance costs due to the additional responsibility of AWS. Insurers may require a "no-touch" policy as a condition of coverage. Airport operators should consult with their risk managers to review:

- Current insurance policies that may cover AWS
- An umbrella policy or increased liability coverage
- Exclusions and conditions affecting AWS

REFERENCES

Airports Council International – North America (2023, August). *ACI-NA position on TSA's Aviation Worker Screening National Amendment.* https://airportscouncil.org/wp-content/uploads/2023/08/ACI-NA-USPC-Position-on-TSA-Aviation-Worker-Screening-Mandate.pdf

American Association of Airport Executives (2023, August). *AAAE Urges TSA to Rescind ASP Amendment on Aviation Worker Screening*. https://aaae.org/lastest-from-washington/federal_80923

Code of Federal Regulations (2024, May). *Title 49 Chapter B.* https://www.ecfr.gov/current/title-49/subtitle-B/chapter-XII/subchapter-C/part-1540/subpart-B?toc=1

International Civil Aviation Organization, *DGP-WG/06-WP/50 Appendix A*. https://www.icao.int/safety/DangerousGoods/Working%20Group%20of%20the%20Whole/WP.50.AppA1.pdf

Long, J (2017). *Importance of Airport Stakeholder Outreach.* Aviation Pros: https://www.aviationpros.com/airports/blog/12388063/importance-of-airport stakeholder-outreach

Transportation Security Administration (2024, May). *Screening Partnerships Program*. https://www.tsa.gov/for-industry/screening-partnerships

APPENDIX A: PROHIBITED ITEMS PERMIT APPLICATION

Example from Section 6.2.1.

PROHIBITED ITEMS EXCEPTION PERMIT

Legal Last Name	Legal First Name
Legal Middle Name	Employee UPID Number (First number listed on POS ID Badge)
Company Name	Printed Name of Authorized Signer
Home Phone/Cell Phone	Email

THIS POLICY MUST BE REVIEWED AND BRIEFING MUST OCCUR BEFORE PERMIT ISSUED

PROHIBITED ITEMS POLICY

I will comply with all rules and regulations, guidelines, and policies concerning airport security and the use of the security badge. Any non-compliance may result in the suspension or revocation of the privilege of having the security badge as well as any civil or criminal penalties as allowed by Federal, State, or Local Law.

By signing this permit request:

- I understand that this permit is an exception to the prohibited items policy and I understand it is a privilege and not a guaranteed right as an ID Badge Holder.
- I have reviewed the TSA Prohibited Items list, and I understand that I am responsible for all tools & equipment that I take into the secured or sterile areas of the Airport, and that they will remain under personal care or lock and key at all times.
- I understand that I will be held liable for any tools, supplies or equipment left abandoned and will be subject to penalties per the Security Violations Handbook and identified in . I confirm that the tools and equipment that I am bringing into the secured or sterile areas of the Airport are for my work duties specific to my job assignments.

ID Badge holders are specifically subject to inspection/screening by the : or Transportation Security Administration when accessing, or present within, the secured or sterile area of the Airport. The inspection/screening may extend to both the ID Badge holder's person and property. I understand that I may be subject to such inspection/screening, acknowledge that my consent to such an inspection/screening is a condition for the : to issue me an ID Badge, and I agree to submit to and cooperate with such an inspection/screening if requested. I further acknowledge that the failure to submit to, or cooperate with, such an inspection/screening may result in the immediate suspension and revocation of my ID Badge.

If the security badge is lost, stolen or damaged, I understand that I must report the occurrence to the Credential Center **IMMEDIATELY**. Outside of regular business hours, contact

I understand and agree to abide by all policies regarding the responsibility of ID Badge Holders and the ID Badge Holder Agreement I signed when applying for the ID Badge. I understand that this permit may also be revoked at any time.

I hereby affirm that I have read the Prohibited Items Policy, reviewed the prohibited item list, and I understand and accept all the rules and regulations of the agreement. I understand that I will be held liable for all information in the above agreement.

Applicant Signature (Must be in Ink)	Date
Authorized Signer (Must be in Ink)	Date